

IN THE CLAIMS

Please amend claims 1, 5 and 9 as indicated below.

This listing of claims will replace all prior versions, and listings, of claims in the application.

**Listing of Claims:**

Claim 1 (currently amended) A method for securing alterable data in a remotely managed system comprising the steps of:

    providing protected storage accessible only by Basic Input Output System (BIOS) code;

    storing a symmetrical encryption Key in said protected storage;

    encrypting normally unaccessible (NA) data with said symmetrical encryption Key; and

    storing said encrypted NA data and accessible non-encrypted (ANE) data in an unprotected electronically erasable programmable read only memory (EEPROM) with existing write protect algorithms.

Claim 2 (original) The method of claim 1 further comprising the steps of:

    altering said ANE data by issuing an existing write request to said BIOS from said write protect algorithms for said EEPROM; and

    updating said ANE data in said EEPROM.

Claim 3 (original) The method of claim 1 further comprising the steps of:

    accessing said NA data via a change request issued to said BIOS over a secure communication link;

    validating said change request;

    retrieving said symmetrical encryption Key by said BIOS in response to said validated change request;

    using said symmetrical encryption Key to decrypt and alter said NA data;

    encrypting said altered NA data using said symmetrical encryption Key; and

storing said altered encrypted NA data in said EEPROM.

Claim 4 (original) The method of claim 1 further comprising the steps of:  
hashing said ANE data and encrypting said Hash with said symmetrical encryption Key;  
storing said encrypted Hash with said ANE data;  
computing a Hash of configuration data in said ANE data on a boot-up request;  
decrypting said stored encrypted Hash of said configuration data;  
comparing said decrypted Hash of said stored configuration data to said computed Hash of said configuration data from said ANE data;  
booting normally in response to a compare of said decrypted Hash and said computed hash; and  
issuing tamper notification and initiating recovery processes on a non-compare of said decrypted Hash and said computed hash.

Claim 5 (currently amended) A computer program product for securing alterable data in a remotely managed system with minimal secure storage, said computer program product embodied in a machine readable medium, including programming for a processor, said computer program comprising a program of instructions for performing the program steps of:

providing protected storage accessible only by Basic Input Output System (BIOS) code;  
storing a symmetrical encryption Key in said protected storage;  
encrypting normally unaccessible (NA) data with said symmetrical encryption Key; and  
storing said encrypted NA data and accessible non-encrypted (ANE) data in an unprotected electronically erasable programmable read only memory (EEPROM) with existing write protect algorithms.

Claim 6 (original) The computer program product of claim 5 further comprising the program steps of:

altering said ANE data by issuing an existing write request to said BIOS from said write protect algorithms for said EEPROM; and  
updating said ANE data in said EEPROM.

Claim 7 (original) The computer program product of claim 5 further comprising the program steps of:

accessing said NA data via a change request issued to said BIOS over a secure communication link;  
validating said change request;  
retrieving said symmetrical encryption Key by said BIOS in response to said validated change request;  
using said symmetrical encryption Key to decrypt and alter said NA data;  
encrypting said altered NA data using said symmetrical encryption Key; and  
storing said altered encrypted NA data in said EEPROM.

Claim 8 (original) The computer program product of claim 5 further comprising the program steps of:

hashing said ANE data and encrypting said Hash with said symmetrical encryption Key ;  
storing said encrypted Hash with said ANE data;  
computing a Hash of configuration data in said ANE data on a boot-up request;  
decrypting said stored encrypted Hash of said configuration data;  
comparing said decrypted Hash of said stored configuration data to said computed Hash of said configuration data from said ANE data;  
booting normally in response to a compare of said decrypted Hash and said computed hash; and  
issuing tamper notification and initiating recovery processes on a non-compare of said decrypted Hash and said computed hash.

Claim 9 (currently amended) A computer system comprising:

a central processing unit (CPU);  
a random access memory (RAM);  
an electronically erasable programmable read only memory (EEPROM);  
an I/O adapter; and  
a bus system coupling said CPU to said EEPROM, said I/O adapter, and said RAM, wherein said CPU further comprises:  
protected storage accessible only by Basic Input Output System (BIOS) code;  
circuitry for storing said symmetrical encryption Key in a protected storage;  
circuitry for encrypting normally unaccessible (NA) data with said symmetrical encryption key; and  
circuitry for storing said encrypted NA data and accessible non-encrypted (ANE) data in a non-protected electronically erasable programmable read only memory (EEPROM) with existing write protect algorithms.

Claim 10 (original) The data processing system of claim 9 further comprising:

circuitry for altering said ANE data by issuing an existing write request to said BIOS from said write protect algorithms for said EEPROM; and  
circuitry for updating said ANE data in said EEPROM.

Claim 11 (original) The data processing system of claim 9 further comprising:

circuitry for accessing said NA data via a change request issued to said BIOS over a secure communication link;  
circuitry for validating said change request;  
circuitry for retrieving said symmetrical encryption Key by said BIOS in response to said validated change request;  
circuitry for decrypting and altering said NA data said using said symmetrical encryption Key;  
circuitry for encrypting said altered NA data using said symmetrical encryption Key; and

circuitry for storing said altered encrypted NA data in said EEPROM.

Claim 12 (original) The data processing system of claim 9 further comprising:

- circuitry for hashing said ANE data and encrypting said Hash with said symmetrical encryption Key;
- circuitry for storing said encrypted Hash with said ANE data;
- circuitry for computing a Hash of configuration data in said ANE data on a boot-up request;
- circuitry for decrypting said stored encrypted Hash of said configuration data;
- circuitry for comparing said decrypted Hash of said stored configuration data to said computed Hash of said configuration data from said ANE data;
- circuitry for booting normally in response to a compare of said decrypted Hash and said computed hash; and
- circuitry for issuing tamper notification and initiating recovery processes on a non-compare of said decrypted Hash and said computed hash.